
MergePoint® 53xx Service Processor Manager Firmware

Release Notes

V 1.6.0.10
May 14, 2010

This document includes:

1. Instructions for upgrading
2. Features and enhancements
3. Supported and Tested Service Processors (SPs)
4. Constraints and conditions per SP
5. Constraints and conditions per function
6. Features and enhancements from previous release 1.5.1.12/1.5.2.12

- =====
1. Instructions for upgrading
- =====

Please refer to the MergePoint appliance Installer/User Guide for more information on how to upgrade the MergePoint service processor manager to version 1.6.0.10.

NOTE: If the current version is 1.2.0.13 or earlier, please upgrade to version 1.2.1.07 before upgrading to version 1.6.0.10.

- =====
2. Features and enhancements
- =====

The following features are added or bugs are fixed in this release:

1. Added support for Dell R210, R410, and R710 iDRAC6 Monolithic Servers

NOTE: If the DSView 3® software is used with the MergePoint appliance for this feature, the DSView 3 software must be upgraded to any 3.7.2 version to support this functionality.

Specific iDRAC monolithic servers/firmware versions used in compatibility testing include:

IDRAC6 Monolithic Server	iDRAC Firmware Versions
PowerEdge R210 (iDRAC Express)	1.30 (Build 24)
PowerEdge R410 (iDRAC Express)	1.30 (Build 24)

IDRAC6 Monolithic Server	iDRAC Firmware Versions
PowerEdge R710 (iDRAC Express)	1.30 (Build 24)
PowerEdge R710 (iDRAC Enterprise)	1.30 (Build 24)

iDRAC Express models do not provide vKVM capability or power statistics information. The MergePoint appliance suppresses the web interface control of these features. DSView 3 software will present the Power Statistics tool for iDRAC Express models, but this tool provides undefined results and should not be used.

2. Added support for IBM IMM-based Monolithic and Blade servers

NOTE: If the DSView 3 software is used with the MergePoint appliance for this feature, the DSView 3 software must be upgraded to any 3.7.2 release to support this functionality.

Specific IMM monolithic servers/firmware versions used in compatibility testing include:

IMM-based Monolithic Server	IMM Firmware Versions
IBM System x3550 M2 (7946)	YUOO48D
IBM System x3650 M2 (7947)	YUOO48D
IBM System x iDataPlex dx360 M2 server (7321)	YUOO48D

Specific IMM blade servers/firmware versions used in compatibility testing include:

IMM-based Monolithic Server	IMM Firmware Versions
IBM BladeCenter HS22 (7870)	YUOO48F

IMM Standard models do not provide vKVM capability. The MergePoint appliance web interface displays the vKVM selection, and the IMM Web interface notifies the user if vKVM is not supported on the target server.

3. Added Power Monitoring and Serial Session support for Dell iDRAC Blade Servers

For iDRAC blade servers which are directly discovered and managed similar to monolithic servers, Power Monitoring information, including Cumulative Power, Peak Power, Peak Amperage and Telnet and SSH serial session interfaces are now available through the MergePoint appliance.

4. Improved Special Character Password Handling

Improvements to handling of passwords containing special characters used during SP discovery and management are included. These improvements apply to all SP types but were specifically intended for HP iLo.

Further improvements related to special character passwords in DirectCommand autologin for several SP types are also included.

Note that IBM has recently addressed issues related to special character passwords in their RSA-II SP firmware for the IBM 3950. We recommend upgrading the SP firmware to version A3EP40A or later if password issues occur.

5. Enabled TACACS Authentication

Authorization for remotely authenticated users, including TACACS, is now enabled by the addition of a role attribute for user groups. Remotely authenticated users whose remote configured group matches a group created on the MergePoint appliance are assigned the roles and devices of that MergePoint appliance user group at the appliance login.

6. Corrected Static Route definition

The MergePoint appliance can now correctly accept a static route IP address that is longer than 13 characters.

7. Improved SP Discovery

Discovery of the following SPs now performs correctly when authenticated using one of the credentials on the Default SP Users list:

- IBM RSA II and IMM monolithic and blade Servers
- Dell M600, M605, M610, M710, M805, R210, R410 and R710 servers
- Sun ALOM servers

See the MergePoint appliance Installer/User Guide for how to manage the Default SP Users list.

8. Improved Auto-discovery and management of ELOM SPs

The MergePoint appliance can now automatically discover and automatically manage ELOM SPs if the username/password credentials for the target service processors are in one of the first three entries of the Default SP Users list. Otherwise, the ELOM will lock out access and the target service processors will not be added.

9. Improved SNMP configuration

Renaming a service processor alias after an SNMP Proxy has been configured so that SP will no longer affect the SNMP Proxy operation.

Configuring an SP SNMP Proxy via the Command Line Interface

The following example assumes an SP at IP address 10.207.16.73 with an alias name "IMM" that has its own SNMP community name of "public1." This SP should be accessed by the public community name "mp_sp1" on the MergePoint appliance.

a) If an existing view is not defined, create one:

```
> add snmpd view SpView
> set snmpd view SpView 0 incl_excl included subtree .1.3.6.1
```

b) Create the SNMP SP Proxy

```
> add snmpd proxy 10.207.16.73
> set snmpd proxy 10.207.16.73 context IMM version 1 community public1 oid .1.3
```

c) Define the access settings

```
> add snmpd com2sec mp_sp1
> set snmpd com2sec mp_sp1 name <username> context IMM
```

```
> add snmpd group <groupname>
> set snmpd group <groupname> sec_model v1 sec_name <username>
> add snmpd access <groupname> IMM
> set snmpd access <groupname> IMM noauth read <viewname>
```

where <groupname> = gmp_sp1, <username> = cmp_sp1 and viewname = SpView.
The groupname must begin with 'g' and the username must begin with 'c'

d) Apply the changes

```
> commit
> exit
```

Read the SP MIB from an SNMP management application using the public community name "mp_sp1"
(e.g.,
\$> snmpwalk -v 1 -c mp_sp1 <mp_ip_address>)

Support Issues addressed in this release:

65578538 65556433 65554651

3. Supported and Tested Service Processors (SP)

The following SPs (shown in alphabetical order) are supported in this release. Note that every SP model and firmware version has not been verified, so some incompatibilities with particular models may be seen.

Service Processor	Notes
Dell® DRAC 3	
Dell DRAC 4	
Dell DRAC 5	Tested PowerEdge 2950 with DRAC5 firmware version 1.45.
Dell 10G	Tested R805v running firmware version 1.44.
Dell BladeCenter DRAC/MC	Tested with firmware version 1.3 (build 06.12).
Dell M1000e Chassis	Tested with CMC firmware versions 1.30, 2.00, and 2.11.
Dell iDRAC Blade Server:M600	Tested with iDRAC firmware versions 1.20 (Build 11), 1.40 (Build 12) and 1.50 (Build 13).
Dell iDRAC Blade Server:M605	Tested with iDRAC firmware version 1.1 and 1.51 (Build 0).
Dell iDRAC Blade Server: M610	Tested with iDRAC firmware version 2.0.0 (Build 28), 2.02 (Build 4) and 2.10 (Build 33).

Service Processor	Notes
Dell iDRAC Blade Server: M710	Tested with iDRAC firmware version 2.02 (Build 4) and 2.10 (Build 33).
Dell iDRAC Blade Server: M805	Tested with iDRAC firmware version 1.40 (Build 12) and 1.51 (Build 0).
Dell iDRAC6 Monolithic Server R210	Tested with iDRAC firmware version 1.30 (Build 24).
Dell iDRAC6 Monolithic Server R410	Tested with iDRAC firmware version 1.30 (Build 24).
Dell iDRAC6 Monolithic Server R710	Tested with iDRAC firmware version 1.30 (Build 24).
Fujitsu iRMC	Tested BX600S2 with iRMC firmware version 2.21G.
Fujitsu iRMC S2	Tested RX200 S4 and RX300S4 with iRMC2 firmware version 3.44A.
HP® IPMI	Tested DL140 with IPMI 2.0 firmware version 2.12.
HP iLo	Tested DL585 with iLo firmware version 1.84.
HP iLo2	Tested DL385G2 with iLo2 firmware version 1.42. Also, DL320 tested with v1.79, DL365 tested with v1.70, DL360 tested with v1.79, DL585G2 tested with v1.70 and DL580G5 tested with v1.77.
HP BladeSystem	Tested with OA firmware version 1.30 and iLo2 blade firmware version 1.22.
IBM® RSA II	Tested 3550 with firmware version GFEP33B, 3650 with firmware version GGEP36B and 3950 with firmware version A3EP36B and A3EP41B.
IBM dx360 M2 (IMM)	Tested model 7321AC1 with firmware version YUOO48D.
IBM x3550 M2 (IMM)	Tested model 7947AC1 with firmware version YUOO48D.
IBM x3650 M2 (IMM)	Tested model 79463AU with firmware version YUOO48D.
IBM BladeCenter®	The BladeCenter Management Module (BCMM) is not supported, but its successor the Advanced Management Module (BCAMM) is supported. Tested with firmware versions BPET48N, BPET48Q and BPET50G. Also tested BPET50K with IMM blades.
IPMI 1.5	
IPMI 2.0	
SUN® ILOM	Standalone SUN servers only. Blade servers not supported in this release. Tested with ILOM firmware version 2.0.2.6 build 35128.

Service Processor	Notes
SUN ALOM	Standalone SUN servers only. Blade servers not supported in this release. Tested Fire Netra 240 with ALOM firmware version 1.6.9.
Sun ELOM	Tested Fire x2200 M2 with ELOM firmware version 3.20.

=====

4. Constraints and conditions per SP (in alphabetical order)

=====

Dell DRAC3, DRAC4 and DRAC5

1. If a Java Applet in the web browser running on a Linux client does not have privileges to listen on Port 443 of the local IP address (127.*.*), the DRAC3 DirectCommand functions will not be functional. Please insure that the listen privilege is available for port 443.
2. When the maximum number of sessions in DRAC4 or DRAC5 has been reached, a new Autologin or vKVM DirectCommand session will fail. The failure can be recovered by resetting the SP via Telnet or SSH. The command for SP reset is "racadm racreset".
3. If DirectCommand launches for DRAC5 servers are unsuccessful, ensure that the JRE is set to allow temporary file storage and that previous temporary files are deleted through the Java Control Panel.
4. Sometimes, vKVM DirectCommand launches for DRAC5 servers are unsuccessful and only show a blank screen when running from the Firefox browser. In this case, we have seen successful operation using the IE browser when running DRAC5 version 1.20 and 1.45. When DRAC5 version 1.45 is used, vKVM can be launched under Firefox by launching Autologin DirectCommand, then browsing to the Remote Console to initiate vKVM through the DRAC5 native web interface.
5. The DRAC5 does not support use of the forward slash in login passwords. Avoid use of the forward slash in password definition.

Dell DRAC/MC and Blades

1. The vKVM/VM operations for the DRAC/MC blades initiated through a DirectCommand browser session will function properly only if the client can directly communicate with the native SP web interface.
2. Sometimes, Autologin DirectCommand operation to DRAC-MC servers does not complete and either displays the message "Internet Explorer cannot display the webpage" for the Internet Explorer 7 browser, or displays a blank page for the Firefox 3 browser. The Autologin DirectCommand operation has been observed to complete if the page is refreshed.

Dell M1000e CMC

1. The M1000e native web interface cannot be opened using the Firefox 3 browser, which also affects the browser link within the MergePoint appliance when using the Firefox 3 browser. Instead, the Autologin DirectCommand option can be used, or Internet Explorer 7 can be used as the browser.
2. M1000e Autologin DirectCommand sessions are not automatically restarted upon session timeout. Click the Autologin DirectCommand link again to restart the session.
3. The M1000e "Single Sign-in" functionality cannot be supported when logged in using the Browser DirectCommand login. Use Autologin DirectCommand for this functionality.

-
4. When connecting to an iDRAC blade using the M1000e "Single Sign-in" feature, the blade's vKVM connection is only functional if the default vKVM ports are configured in the blade. If the vKVM ports are redefined, then vKVM is only supported through a DirectCommand session to the blade.
 5. The CMC web interface login selection within the iDRAC blade web interface is not accessible through the MergePoint appliance. Instead, the M1000e Autologin DirectCommand option should be used to access the CMC web interface.
 6. The login process for the M1000e may take up to 20 seconds after proper username and credentials are presented and therefore it may take several seconds to access some features in the MergePoint appliance web interface (e.g., displaying power information may take 15-20 seconds for an M1000e chassis.)
 7. The Dell M1000e CMC chassis requires that all servers within the chassis must first be turned off successfully before the chassis can be turned off. Please follow this sequence when controlling the CMC power through the MergePoint appliance to avoid inconsistent behavior in power states and/or error messages.
 8. When controlling power for a Dell M1000e blade server through the MergePoint appliance web interface, the power operation will be issued successfully but an error message of "SP action failed" will appear on the power status update. This error message can be ignored. Refresh the screen to correctly display the updated power status.

Dell iDRAC Blades

1. Occasionally, Autologin DirectCommand attempts to connect to an iDRAC blade are rejected, and a DirectCommand Applet Error is presented that contains an error string from the blade, such as "Failure_Session_Creation." Workarounds include retrying the Autologin DirectCommand operation after a few minutes, retrying blade login through the chassis Single Sign-in feature, or resetting the blade.
2. Sometimes after a session expires, the iDRAC blade logout selection is not processed. If this occurs, close the browser window or tab.
3. The login session associated with an iDRAC blade vKVM session is not automatically terminated and must be allowed to time out.
4. Some anomalies have been seen with the Dell M610 blade when it is either directly managed or managed through the MergePoint appliance. These anomalies include:
 - a. The default root/calvin uid/password does not always allow access, yet another defined username does seem to work.
 - b. Virtual Media does not connect.

Please check the Dell web site for release note updates.

Dell iDRAC6 Monolithics and Blades

1. A SoL error message, "Payload already active on another session," will occur on a MergePoint appliance attempting to manage a Dell iDRAC that is already being managed by another MergePoint appliance.
2. To disable the SoL function for any iDRAC SP, complete the following steps from the MergePoint appliance web interface:
 - a. Select *Configuration - Serial over LAN*, and then uncheck *Enable Serial Over LAN* to disable SoL and click *Apply*.
 - b. Select *System - Advanced Tools*, and then click *Cold Reset*.
 - c. After the SP reset is complete, attempt to open a SoL session to verify no activity.

To enable the SoL function on an iDRAC SP, complete the following steps from the MergePoint appliance web interface:

- a. Select *Configuration - Serial over LAN*, and then check *Enable Serial Over LAN* to enable SoL and click *Apply*.

-
3. When no Trap Setting Destinations are enabled on the native SP web interface for iDRAC SPs, clicking the *Event Destination* tab in the MergePoint appliance web interface will indefinitely display the message "Request in process. Please wait." To avoid this, enable at least one Trap Setting Destination through the native SP web interface.

FTS iRMC, iRMC S2

1. If Autologin DirectCommand operations for iRMC2 servers present an additional login prompt or are otherwise unsuccessful, ensure that the JRE is set to disallow temporary file storage and that previous temporary files are deleted through the Java Control Panel.
2. iRMC S2 SPs that use login passwords containing the ampersand character cannot be discovered or managed by the MergePoint appliance. The SP can be discovered and managed when the login passwords do not contain the ampersand character.

HP iLo, iLo2

1. The iLO2 vKVM runs with ActiveX in an Internet Explorer browser and with a Java applet in other browsers such as Firefox 3. The vKVM with ActiveX integrates Virtual Media, while vKVM with a Java applet does not. Multi-session operation is not supported for vKVM DirectCommand operations in the Internet Explorer browser.
2. Clearing IML for iLO 1 is not currently supported through the MergePoint appliance web interface. The activation button appears for both iLO 1 and iLO 2 SPs, but is only functional for iLO 2 SPs.
3. The iLO 2 does not support use of the single or double quotation marks in login passwords. Avoid use of quotation marks in password definition.

HP BladeSystem and blades

1. The vKVM/VM operations for the HP blades initiated through a DirectCommand browser or Autologin session will function properly only if the client can directly communicate with the native SP web interface.
2. The HP blades managed under HP BladeSystem OA are not accessible when running under DirectCommand. These HP blades must be discovered and managed separately from the BladeSystem for DirectCommand functionality.
3. In limited testing with the HP BladeSystem OA version 1.81, it was noted that blade power, sensor and SoL operations are not functional when the blade is managed through the OA. These operations are functional when the iLo blade is discovered and managed separately from the BladeSystem.

IBM RSA-II

1. When a vKVM session is connected on an RSA-II server, a second login with the same userid will cause the original vKVM session to be disconnected. This includes a second login through the MergePoint appliance which will use the same userid. This behavior is by design in the RSA-II servers.
2. Intermittent load failures of the vKVM and VM applets on RSA-II servers are seen when the JRE is allowed to keep temporary files on the computer. When using these vKVM and VM applications on RSA-II servers, Avocent recommends setting the JRE to disallow temporary file storage through the Java Control Panel.
3. vKVM operation to RSA-II servers launched through a DirectCommand browser login session may not be successful. Avocent recommends using the DirectCommand Autologin operation.
4. vKVM operation to RSA-II servers is incompatible with JRE-6u13. Avocent recommends using JRE-6u11 or JRE-6u14 or later for these applications.

-
5. When managing RSA-II servers through a MergePoint appliance using the DSView 3 software, DirectCommand sessions sometimes cannot be successfully launched when using JRE versions above 6u7 without disabling “the next-generation Java Plug-in” setting through the Java Control Panel. If these issues continue to occur while disabling “the next-generation Java Plug-in,” Avocent recommends downgrading the JRE to 6u7.
 6. The native web interface for the IBM 3950 RSA-II server will not allow login if the password contains special characters unless the SP firmware is upgraded to A3EP40A or later. Please upgrade the SP firmware to use special characters passwords with DirectCommand functionality.

IBM BladeCenter and Blades

1. The IBM BladeCenter native web interface provides access to vKVM and vMedia functions for its blades. DirectCommand operations for blades should be initiated through the BladeCenter interface.
2. Autologin and vKVM DirectCommand operations for the IBM BladeCenter fail by presenting a login prompt when the BladeCenter is automatically discovered and/or managed. To establish Autologin DirectCommand functionality, please delete the BladeCenter from the MergePoint appliance web interface and then manually add it back into the appliance.

IBM IMM Monolithics

1. The vKVM DirectCommand sessions for IMM-based monolithic servers do not successfully launch on some IE7 and IE8 installations. To correct this issue from the IE browser menu, select *Tools*, then *Internet Options*, then select the *Security* tab and click the *Custom Level* button. Scroll down to the Downloads settings group and click the *Enable* radio button for the “Automatic prompting for file downloads” setting.
2. IMM-based monolithic servers purchased with the “IMM Standard” option do not support vKVM. The MergePoint appliance cannot detect the “IMM Standard” configuration prior to web interface login, so the user is not notified until after the vKVM login attempt.
3. Occasionally, Autologin and vKVM DirectCommand sessions for IMM-based monolithic servers do not successfully launch when switching the session launch between the DSView 3 software and the MergePoint appliance web interface. Clear the browser cache and re-launch the session if this situation occurs.
4. The IMM Monolithic servers do not support use of the special characters ':', '&', '\', and '<' in login passwords. Avoid use of these characters in password definition.

IPMI1.5 / IPMI 2.0

1. IPMI1.5 or IPMI2.0 servers have no native management web interface by default, but these servers can be integrated with a web interface. In this case, a user-defined SP profile can be created for the IPMI SP with the appropriate web port and web scheme to enable the DirectCommand “Browser session” option in the MergePoint appliance web interface.

Sun ALOM, ELOM, ILOM

1. ALOM servers have no native management web interface by default, but these servers can be integrated with a web interface. In this case, a user-defined SP profile can be created for the ALOM SP with the appropriate web port and web scheme to enable the DirectCommand “Browser session” option in the MergePoint appliance web interface.
2. The ELOM native web interface vKVM operation may conflict with other network services commonly run on server machines. If conflicts occur, we suggest performing these operations on a workstation computer instead of a server computer.

-
3. The ILOM KVM/VM applet requires the username and password to be entered manually.
 4. ELOM and ALOM SPs that use login passwords containing special characters cannot be discovered or managed by the MergePoint appliance. These SPs can be discovered and managed when the login passwords do not contain special characters.

=====

5. Constraints and Conditions by function

=====

This release includes the following constraints or conditions by the functions (listed in alphabetical order) below.

DirectCommand

1. Browser session functionality is implemented as pure port forwarding. The web interfaces of some SPs may work abnormally in this mode regardless of the port forwarding implementation. For example, sometimes DirectCommand session options are not presented after enabling DirectCommand through the MergePoint appliance web interface when running the Firefox 3.5 browser. If this occurs, Avocent recommends downgrading to the Firefox 3.0 browser.
2. If login prompts are presented during Autologin DirectCommand sessions, the login username/password associated with that SP and stored within the MergePoint appliance may need to be re-entered.
3. DirectCommand is currently not supported for JRE-6u18 and up. For full DirectCommand functionality, use a previous JRE version.
4. If a DirectCommand session launch fails with an "Unable to launch the application" message, please try either:
 - a) Downgrading the Java version to JRE-6u11 or earlier
 - b) Unchecking the *Enable the next-generation Java Plug-in* checkbox in the Java control panel

Discovery and Management

1. The MergePoint appliance supports an alias for every type of SP. Do not use special characters in the alias. Only the following characters are allowed: "0-9", "a-z", "A-Z" and "-".
2. With respect to automatic management, some interactions are particular to specific service processors. Some service processors will not allow over three attempts to login with incorrect credentials. Upon exceeding the number of allowed attempts, the service processor will not allow anymore attempts within a given period of time. Therefore, it is best practice to only specify usernames and passwords that are necessary under the Default SP Users tab. For instance, an iLO service processor will allow two attempts before disabling its interface for 60 seconds, and should have its username and password entered first. It may, therefore, be necessary to delete existing default usernames and passwords before adding iLO usernames and passwords. Also, the automatic management feature should be turned on before creating the discovery ranges. This feature can be turned on under the System tab of the MergePoint appliance web interface.
3. Discovery range status may not be available immediately after rebooting the MergePoint appliance. It may take an additional 30 seconds before the Discovery range settings can be changed via the MergePoint appliance web interface, WS-Man and CLP. This time window only occurs after rebooting or resetting the appliance.

Network Configuration

1. BMC Provisioning can only be configured on the secondary Ethernet Interface (eth1).
2. Please note that the MergePoint appliance reserves 192.168.0.10 and 192.168.0.20 as default addresses for eth0 and eth1 respectively. To configure a private subnet using the 192.168.0.x address range, the eth0 and eth1 addresses must be moved from this range. If IP address conflicts occur after reconfiguring, please contact Avocent Technical Support.
3. If a pre-configured hostname for an SP is delivered to the MergePoint appliance DHCP server, this pre-configured hostname will be used as the default alias name. If no hostname is specified, the IP address will be used as the default alias name.
4. DHCP will only operate with one private subnet defined. If the user wishes to define another private subnet for use with DHCP, the original private network must be deleted before the new private subnet is defined, and a reboot of the MergePoint appliance occurs.
5. Occasionally, a MergePoint appliance configured with a static IP address may revert to a dynamic IP address following a web upgrade. Please reboot the MergePoint appliance to restore the static IP address.
6. When using PXE provisioning and DHCP assigned addresses, both services should not be executing simultaneously. This action may cause the DHCP service to errantly assign an address for which the PXE provisioning service is responsible and vice versa.

Serial-over-LAN (SoL)

1. The "Ctrl+c" interrupt is inactive during SoL sessions using MindTerm and will not pass to the SP.
2. Certain SPs output some history information by default during the opening of a SoL session. Be sure that any scripts written are expecting this extra information.

SP Operations

1. When a user-defined SP profile is used, some MergePoint appliance web interface functionality in the Configuration tab normally seen for the SP default profile may be missing. If this behavior is not desired, the SP default profile may be used.
2. The MergePoint appliance web interface does not provide enable/disable options per Event Destination IP address. This control should be performed using the native SP web interface.
3. Occasionally, a new Native IP connection will appear twice on the Connects list of the MergePoint appliance web interface. This second entry has no effect and can either be deleted or ignored.
4. Occasionally, the Configuration/Event Destination page may be displayed with missing fields and an error message. In this case, a communication error with the SP has occurred. The communication may be reattempted by browsing away from this page, then returning. If the error continues, the SP needs to be reset.

Miscellaneous

1. Usernames under User Configuration must be all in lowercase letters.
2. An SNMP group created through the CLI of the MergePoint appliance does not appear in the web interface of the appliance. Please use either only the CLI or only the web interface to manage SNMP groups.

Upgrading and Restoring

1. Power outage during the upgrading process is not recoverable and the MergePoint appliance may not restart after this occurs.

-
2. Data import should only be made into a MergePoint appliance running the same firmware version used when the data was exported. Therefore, the import process should be:
 - a. Upgrade the MergePoint appliance from which the data will be exported to the necessary firmware version.
 - b. Export the data from the upgraded MergePoint appliance.
 - c. Upgrade the second MergePoint appliance to which data will be imported using the same version as the MergePoint appliance that exported the data.
 - d. Import the data to the second MergePoint appliance.

=====

6. Features and enhancements from previous release 1.5.1.12/1.5.2.12

=====

The following features are added or bugs are fixed in this release:

1. Added Automatic Management of DHCP devices and Discovered Devices

A new section of device management options has been added to the Settings page under the System tab. These options enable or disable automatic management of a DHCP device and automatic management of discovered devices.

2. Changes to discovery

- There is more reliance on ipmitool and expect scripts for discovery in this release. Care must be taken to ensure that target servers are configured correctly. Each potential target server must have IPMI over LAN and SSH enabled if offered as a configurable option.
- While allowing more server types, more accuracy and better security, ipmitool and expect scripts can be time consuming and can also cause the SP to lock out the discovery process if too many login attempts are made with non-matching username/password combinations. Therefore, it is important to minimize the number of usernames and passwords on servers that will be discovered. Before discovery takes place, the Default SP Users list in the MergePoint appliance web interface should be cleared of all logins that are not needed.
- IBM® Blade Center and RSA servers are now discovered using expect scripts and the SSH protocol. RSA devices are discovered both with and without SoL support. The expect scripts attempt each of the logins in the Default SP Users list until the SP type is verified.
- Dell® DRAC 5 and iDrac blade servers are now discovered using ipmitool instead of http POST requests. Instead of using only the default root/calvin login, each login in the Default SP Users list is tried until the SP is verified.
- The order in which different discovery methods are performed has been changed. Before this release, the order was ipmitool, https, telnet, ssh (ALOM only) and IPMI. Now, with full support of the Default SP User logins, ipmitool and SSH expect script discovery are performed for each Default SP User login. If none is found using those methods, then https, telnet and IPMI are performed (in that order).

3. Corrected SP License calculation

The calculation of SP licenses is now correct and matching between the MergePoint appliance and the DSView® 3 management software, whether SPs are added by discovery or manually.

Blades are not counted twice when they are managed both within a chassis and as a standalone SP.

4. Increased Number of Default Username/Password Entries

The maximum number of Default SP Users and corresponding passwords has been increased from five (5) to eight (8) to facilitate support for the number of SPs now available from multiple vendors. Avocent recommends conserving these entries to only configure those needed to discover and/or manually manage their SPs.

5. Improved restore factory process

The default password "Sydney" is now set correctly as the factory defaults are restored. Also, an additional confirmation prompts the MergePoint 5200/5300 SP manager console to "Roll back the version" and to set the menu entry in the MergePoint 5200/5300 SP manager console to "Restore to Factory Defaults." An option is also given to keep or remove the license key(s) from the MergePoint appliance database.

6. Corrected IBM BladeCenter vKVM operation

A DirectCommand vKVM session launched to an IBM BladeCenter running BPET48N firmware will now continue to remain connected until disconnected by the user or by the normal connection timeout.

7. Corrected SP Profile error when adding Sun ALOM

The discovery process now handles a general command-line prompt string that can be site-specific, rather than only processing the default prompt string.

8. Extend LDAP "distinguished name" entry

The "LDAP Base" name specified in the "Authentication Service" section of the MergePoint appliance web interface Wizard tab was extended to 63 characters so that the web interface now matches the underlying firmware capability.

9. SMASH Command Line Protocol (CLP)

The CLP application is set up to use VT100 emulation. Settings for external terminal applications (e.g., PuTTY) are Backspace Key = Delete / Backspace character, Delete key = Escape sequence.

The "--help" argument has been added to the application.

Note: To show the IP address of the MergePoint appliance through the CLP, use the following command: "show -all /map1/ipendpt1." The command listed in the manual does not show the IP address at present.

10. WS-Management

The WS-Management feature has been tested using version 2.1.0 of the openwsman command line client available from <http://www.openwsman.org/project/wsmancli>.

Microsoft WinRM client

If using the WinRM client for Windows® XP or Vista, the following command conversions can be used:

```
> winrm  
enumerate http://sblim.sf.net/wbem/wscim/1/cim-schema/2/AvctMP\_Disc
```

```
overySAP -username:admin -password:admin -r:192.168.96.33:8889/wsman  
-auth:basic
```

```
> winrm get  
"http://sblim.sf.net/wbem/wscim/1/cim-schema/2/AvctMP_DiscoverySAP?  
SystemCreationClassName=AvctMP_ComputerSystem+SystemName=MergePoint  
5300+CreationClassName=AvctMP_DiscoverySAP+Name=OEM Avocent Discove  
ry Serice Access Point1" -username:admin -password:admin  
-r:192.168.96.33:8889/wsman -auth:basic  
  
> winrm set  
"http://sblim.sf.net/wbem/wscim/1/cim-schema/2/AvctMP_DiscoverySAP?  
SystemCreationClassName=AvctMP_ComputerSystem+SystemName=MergePoint  
5300+CreationClassName=AvctMP_DiscoverySAP+Name=OEM Avocent Discove  
ry Serice Access Point1" -username:admin -password:admin  
-r:192.168.96.200:8889/wsman -auth:basic  
@{(oemavocent_startip="192.168.96.50";oemavocent_endip="192.168.96.6  
0"} }
```

AvctMP_DiscoveryService

This class controls general discovery service settings such as the discovery interval. The start/stop method of this class controls the underlying discovery daemon; to start / stop discovery of an IP address range, the AvctMP_DiscoverySAP class should be used instead.

AvctMP_DiscoverySAP

This class controls discovery of a specified IP address range. There are two instances of this class allowing discovery of two separate ranges.

The discovery range start IP address must be greater than the end IP address. If the end address is not currently set, then both addresses must be specified in the same WS-Man command to avoid an error.

Note: There is a spelling mistake in the implementation. For this release, the name "OEM Avocent Discovery Service Access Point" in the manual should be entered as "OEM Avocent Discovery Serice Access Point." This will be corrected in a future firmware release.

Support Issues addressed in this release:

65495719

65524291

65549510

65499019